

⑫ 公開特許公報(A)

昭63-197293

⑪ Int.Cl.⁴

G 06 K 17/00

G 07 F 7/08

識別記号

庁内整理番号

B-6711-5B

L-6711-5B

M-6929-3E

⑬ 公開 昭和63年(1988)8月16日

審査請求 未請求 発明の数 1 (全5頁)

⑭ 発明の名称 ICカード発行システム

⑮ 特 願 昭62-30400

⑯ 出 願 昭62(1987)2月12日

⑰ 発 明 者 神 竹 孝 至 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝総合研究所内
⑰ 発 明 者 阿 部 雅 宏 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝総合研究所内
⑰ 発 明 者 川 村 信 一 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝総合研究所内
⑰ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地
⑰ 代 理 人 弁 理 士 鈴 江 武 彦 外2名

明 細 書

1. 発明の名称

ICカード発行システム

2. 特許請求の範囲

(1) 暗号化された発行情報を記憶する記憶手段と、この記憶手段に記憶された暗号化された発行情報の転送制御を行なう転送制御手段と、この転送制御手段の制御によって転送された前記暗号化された発行情報を復号鍵を用いて復号し、この復号化された発行情報を未発行ICカードに書込む発行情報書込み手段と、この発行情報書込み手段に対してのみ前記復号鍵を与える復号鍵付与手段とを具備したこと特徴とするICカード発行システム。

(2) 前記発行情報書込み手段は、発行用カードリーダー・ライターであることを特徴とする特許請求の範囲第1項記載のICカード発行システム。

(3) 前記復号鍵付与手段は、鍵発生用カードリーダー・ライターと鍵発生用ICカードとからなり、

前記鍵発生用カードリーダー・ライターは、前記鍵発生用ICカードを特定するID番号を出力し、前記鍵発生用ICカードは、該ICカードを特定するID番号を記憶するID記憶回路と、このID記憶回路に記憶されたID番号と前記鍵発生用カードリーダー・ライターから出力されるID番号とを比較する比較回路と、この比較回路での比較結果が一致したら前記復号鍵を送出する復号鍵送出回路とを具備したものであることを特徴とする特許請求の範囲第1項又は第2項記載のICカード発行システム。

(4) 前記発行用カードリーダー・ライターと前記鍵発生用カードリーダー・ライターとは同一筐体に封止密閉されていることを特徴とする特許請求の範囲第3項記載のICカード発行システム。

(5) 前記発行用カードリーダー・ライターと前記鍵発生用カードリーダー・ライターとを共用したことを特徴とする特許請求の範囲第3項記載のICカード発行システム。

3. 発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、カード発行時の安全性を高めた
ICカード発行システムに関する。

(従来技術)

ICカードを発行するには、ID番号、サービス種目、カードの使用可能範囲等の発行情報を未発行のICカードに対して書込む必要がある。この発行情報の中には、ID番号等の守秘を必要とする情報や改ざんされると不正使用されてしまう情報も含まれている。

これに対して、従来のICカード発行システムは、例えば第5図にその概略を示すように、記憶装置1に記憶された発行情報をコンピュータ2の制御のもとでカードリーダー・ライタ3に転送し、このカードリーダー・ライタ3の図示しない挿入部に挿入された未発行のICカード4に対して上記発行情報を書込むことが行われていた。

ところが、このようなシステムでは、不正なプ

せるのではなく、暗号化された発行情報を記憶させ、ICカードに発行情報を書込む発行情報書込み手段は、転送制御手段の制御によって転送された前記暗号化された発行情報を復号鍵を用いて復号し、この復号化された発行情報を未発行ICカードに書込むものとなっている。そして、本発明では、さらに前記発行情報書込み手段に対してのみ前記復号鍵を与える復号鍵付与手段が設けられている。

(作用)

本発明によれば、暗号化された発行情報を復号化するのに使用される復号鍵は、復号鍵付与手段から発行情報書込み手段にのみ与えられるので、復号化は発行情報書込み手段の内部でしか行なうことができない。したがって、もし転送制御装置が不正なプログラムで作動し、記憶手段から発行情報書込み手段に至る経路上で発行情報が盗まれても、これを復号化することができないので、生の発行情報を盗まれたり改ざんされたりすることがない。

プログラムを与えることにより、記憶装置1から出力された生の発行情報をコンピュータ2で書き変える、或は生の発行情報をコピーして保存するという操作をコンピュータ2に行なわせることができる。このため、発行情報を容易に盗んだり改ざんしたりすることが可能であった。

(発明が解決しようとする問題点)

このように、従来のICカード発行システムでは、発行情報の転送制御を司る転送制御手段、例えばコンピュータのプログラムにより容易に発行情報を盗んだり改ざんできるという問題があった。

本発明は、このような問題点を解決すべく考えられたもので、発行情報の転送制御を司る転送制御手段のプログラムをどのように組んでも発行情報が盗まれたり、改ざんされるおそれがないICカード発行システムを提供することを目的とする。

〔発明の構成〕

(問題点を解決するための手段)

本発明は、記憶手段に生の発行情報を記憶さ

(実施例)

以下、本発明の実施例について説明する。

第1図は本発明の一実施例に係るICカード発行システムの構成を示すブロック図である。記憶装置11は、予め図示しない暗号化回路により暗号化された発行情報(暗号発行情報)を記憶する。コンピュータ12は転送制御手段となるものであり、記憶装置11に記憶された暗号発行情報を、発行用の第1のカードリーダー・ライタ13に転送する。第1のカードリーダー・ライタ13は、受入れた暗号発行情報を後述する復号鍵を用いて復号化し、得られた生の発行情報を図示しない挿入部に受入れた未発行の第1のICカード14に書込む。

そして、このシステムには、上記発行用の第1のカードリーダー・ライタ13及び第1のICカード14とは別個に復号鍵付与手段を構成する鍵発生用の第2のカードリーダー・ライタ15と、第2のICカード16とが付加されている。

これら第1、第2のカードリーダー・ライタ13、

15及び第1、第2のICカード14、16は、このシステムにおいてICカードの発行端末17として設けられており、コンピュータ12には、このような発行端末17が例えば通信回線を介して接続されることになる。なお、発行端末17は、各々単一の第1、第2のカードリーダー・ライター13、15からなるものに限定されるものではなく、複数の第1のカードリーダー・ライター13と単一の第2のカードリーダー・ライター15からなる場合、単一の第1のカードリーダー・ライター13と複数の第2のカードリーダー・ライター15とからなる場合、及び各々複数の第1、第2のカードリーダー・ライター13、15からなる場合等、種々の構成をとることができる。

第2図は、上記発行端末17の詳細ブロック図である。第1のカードリーダー・ライター13には、コンピュータ12からの暗号発行情報を復号鍵を用いて復号する復号回路21が設けられている。第1のICカード14には、上記復号回路21で復号化された生の発行情報を入力するためのI/O

ード発行システムにおいて、ICカードの発行手続を行なうには、先ず、未発行状態の第1のICカード14を第1のカードリーダー・ライター13の図示しない挿入部へ、また鍵発生用の第2のICカード16を第2のカードリーダー・ライター15の図示しない挿入部へそれぞれ挿入する。

そして、第1のカードリーダー・ライター13の操作により、コンピュータ12に対して発行作業開始の指示を与えると、コンピュータ12は、記憶装置11から当該ICカード14に関する暗号化された発行情報を読み出し、これを通信回線を介して第1のカードリーダー・ライター13に転送する。

一方、オペレータが第2のカードリーダー・ライター15に対しID番号を入力すると、第2のICカード16の内部でこの入力されたID番号と内部に記憶されたID番号との照合を行ない、両者が一致していれば復号鍵送出回路28から復号鍵が出力される。この復号鍵は、復号回路21に与えられる。

一方、復号回路21には、コンピュータ12に

O回路22と、このI/O回路22を介して入力された発行情報の書き込み制御を司るCPU23と、このCPU23の制御により生の発行情報を記憶するメモリ24とが備えられている。また、第2のカードリーダー・ライター15には、カード発行のためにのみ使用される第2のICカード16を特定するID番号を、例えばオペレータの操作に基づいて送出するID番号送出回路25が設けられている。そして、第2のICカード16には、そのIDカードを特定するID番号を記憶するID番号記憶回路26と、このID番号記憶回路26に記憶されたID番号と、前記ID番号送出回路25から送出されるID番号とを比較し、一致したら一致信号を出力する比較回路27と、この比較回路27からの一致信号を入力して復号鍵を送出する復号鍵送出回路28とを備えている。そして、復号鍵送出回路28から出力される復号鍵は、第2のカードリーダー・ライター15を介して復号回路21に直接与えられている。

以上のように構成された本実施例に係るICカ

より転送された暗号発行情報が与えられている。したがって、復号回路21は、この暗号発行情報を上記復号鍵を用いて復号化する。このようにして復号化された生の発行情報は、I/O回路22、CPU23を介してICカード14の内部のメモリ24に格納される。

以上の手順により生の発行情報がICカード14の内部に格納されることになる。そして、一度メモリ24に格納された発行情報については、読出すことも書き変えることもできない。

本実施例に係るシステムによれば、記憶装置11～コンピュータ12～第1のカードリーダー・ライター13の各経路上の発行情報が暗号化されているので、たとえコンピュータ12に不正なプログラムを与えて発行情報を盗んでも、これを復号化することができない。このため、生の発行情報を知られることはない。また、暗号化された発行情報を改ざんしようとしても、復号鍵が知られない限り、改ざんされた内容に、特定の意味を持たせることができないので、そのような改ざんに

よってICカード14を不正に使用するという企ては成功しない。したがって、このシステムによれば、カード発行時の安全性を高めることができる。特に、このシステムでは、復号鍵付与手段として第2のICカード16を設け、復号鍵をこのICカード16の内部から発生させるようにしているので、第2のカードリーダー・ライター15内に直接復号鍵を入力することによる危険を回避できる。しかも、このシステムでは復号鍵発生のために、ICカード16とID番号の入力とを必要としているので、2重の安全性が図れるなどの効果を奏する。

なお、上記実施例では、発行端末を構成する第1、第2のカードリーダー・ライター13、15を別々に設けたが、第2のカードリーダー・ライター15から第1のカードリーダー・ライター13に与えられる復号鍵が万一盗まれる危険性を考慮した場合には、例えば第3図に示すように、上記2つのカードリーダー・ライター13、15を1つのカードリーダー・ライター31にまとめることが望ましい。この場

合には、例えば2つのカードリーダー・ライターを1つの筐体で封止密閉しておくことが好ましい。

また、発行用カードリーダー・ライターと鍵発生用カードリーダー・ライターとを1つのカードリーダー・ライター32として完全に共用する場合には、第4図に示すように、まず第2のICカード16をカードリーダー・ライター32に挿入して復号鍵を読み出し、続いて第1のICカード13を挿入して発行操作を行なうようにすれば良い。

さらに、以上の各実施例では、復号鍵付与手段として鍵発生用のカードリーダー・ライターと鍵発生用のICカードとを用いたが、このような手段を用いなくても、例えば復号鍵をオペレータ操作で直接入力しても良い。このような構成によっても従来のシステムに比較した安全性向上は十分に見込まれる。

〔発明の効果〕

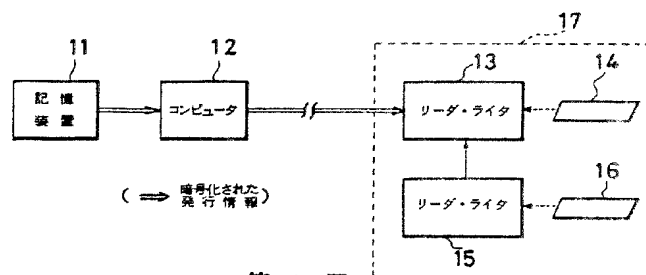
以上述べたように、本発明によれば、記憶手段から転送制御手段を介して発行情報書き込み手段に至る発行情報が暗号化されているので、生の発行

情報が盗まれたり改ざんされるおそれがない。このため、安全性の高いICカード発行システムを提供することができる。

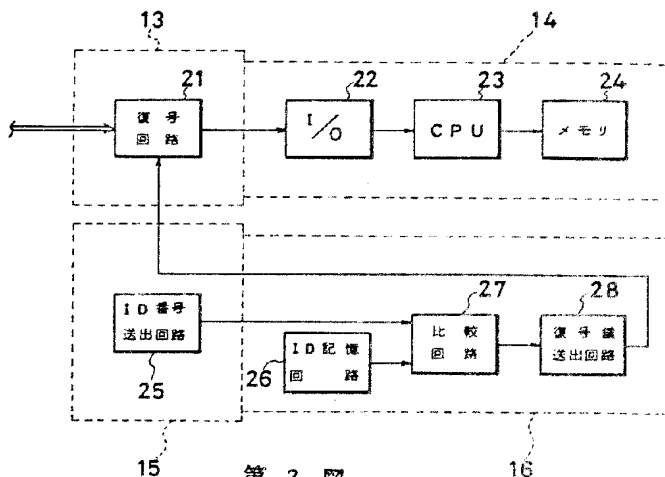
4. 図面の簡単な説明

第1図は本発明の一実施例に係るICカード発行システムの構成を示すブロック図、第2図は同システムにおける発行端末のさらに詳細なブロック図、第3図及び第4図は本発明のそれぞれ他の実施例に係るICカード発行システムの構成を示すブロック図、第5図は従来のICカード発行システムの構成を示すブロック図である。

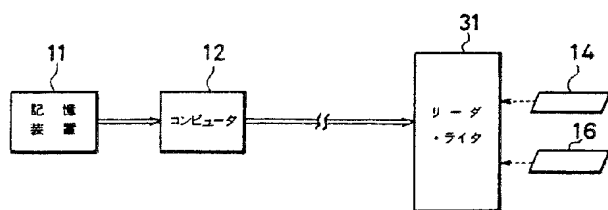
1、11…記憶装置、2、12…コンピュータ、3、31、32…カードリーダー・ライター、13…第1のカードリーダー・ライター、14…第1のICカード、15…第2のカードリーダー・ライター、16…第2のICカード。



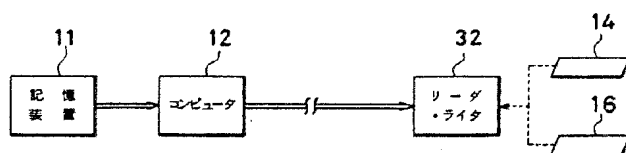
第1図



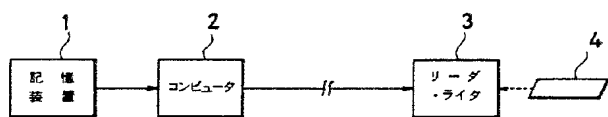
第2図



第 3 図



第 4 図



第 5 図